Preventing Jamming Attacks in Wireless Networks

V. Nagaraju, N. UmaRani

Christu Jyoti Institute of Technology & Science, Colombonagar, Yeshwanthapur, Jangaon, Andhra Pradesh, India

ABSTRACT: This intentional interference with wireless transmissions can be used as a Launchpad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. This paper considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming.

Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing. A sensor is developed that consists of four components. The first is a probabilistic model of the sizes and inter-packet timing of different packet types. The second is a historical method for detecting known protocol sequences that is used to develop the probabilistic models, the third is an active jamming mechanism to force the victim network to produce know sequences for the historical analyser, and the fourth is the online classifier that makes packet type classification decisions. The ratio of the jamming pulses duration to the transmission duration can be as low as 10-4. We investigate and analyse the performance of combining a crypto graphic inter leaver with various coding schemes to improve the robustness of wireless LANs for IP packets transmission [1].

Keywords: jamming, sensor components, wireless network, protocols, Ad hoc networks.

Introduction

Ad hoc networks are envisioned as playing a significant role in mission critical communication for the military, utilities, and industry. An adversary may attempt to attack a victim ad hoc network to prevent some or all victim communication. Such denial-of-service (DoS) attacks have been considered in ad hoc wireless networks at several levels. In this paper we consider encrypted victim networks in which the entire packet including headers and payload are encrypted and thus the attacker cannot directly manipulate any of the victim communication. In this case, the attacker must resort to external physical-layer-based Does, also known as jamming.

Jamming can be as simple as sending out a strong noise signal in order to prevent packets in the victim network from being received. This method of jamming is not the subject of this paper.

This paper attempts to exploit the Protocols at various layers to get three advantages: jamming gain; targeted jamming; and reduced probability of Detection. Jamming gain is the increase in efficiency from exploiting features of the victim network relative to Continuous jamming.

Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications [25], or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats [37]). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. The semethods can only protect wireless transmissions under the external threat

model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broad cast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. he adversary exploits his internal knowledge for launching *selective jamming attacks* in which specific messages of “high importance” are targeted. Jamming can be as simple as sending out a strong noise signal in order to prevent packets in the victim network from being received. This method of jamming is not the subject of this paper. This paper attempts to exploit the protocols at various layers to get three advantages: jamming gain; targeted jamming; and reduced probability of detection. Jamming gain is the increase in efficiency from exploiting features of the victim network relative to continuous jamming.

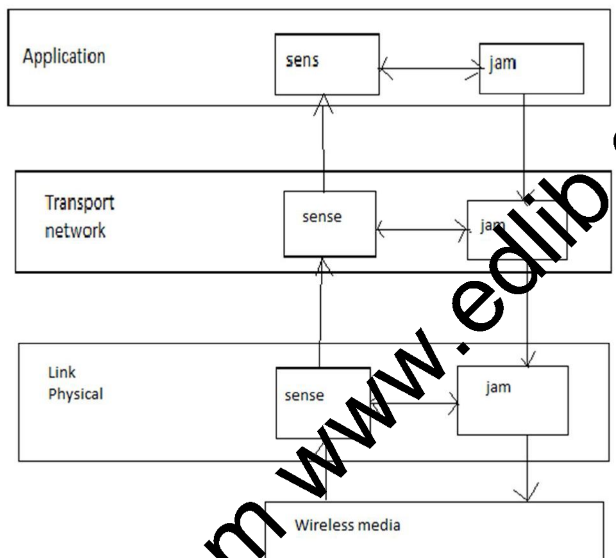

Figure 1 The sensing and jamming layered model

Targeted jamming refers to jamming only specific victim nodes, links, or flows. The attacker may be interested in only certain parts of the victim network, and attacking only these parts can lead to further jamming gains. With reduced probability of detection, the victim network may not realize that jamming countermeasures are necessary. Jamming is not a transmit-only activity. It requires an ability to detect and identify victim network activity, which we denote as *sensing*. At the physical layer a sensor needs to identify the presence of packets. Since the network is encrypted, only the start time and size of the packet can be measured.

1.1 A Layered Model for Jamming

Together jamming and sensing can be broken down into a layered model similar to the OSI stack. We break it down into three levels for convenience as shown in Figure 1. The Link/Physical layer directly interacts with the media. If a higher layer requests a packet to be jammed, then this lower layer generates the physical signal and ensures that a packet and each of its link layer retries are jammed. This layer also provides the basic sensing capability of packet duration and timing.

The Transport/Network Layer interacts with the corresponding Ad Hoc, IP, TCP, and UDP protocols. This layer senses packet types and traffic flows which can then be targeted by jamming. The Application layer senses HTTP sessions, VoIP set up and the like and targets specific user activities for jamming.

2. Problem Statement and Assumptions

2.1 Problem Statement

Consider the scenario depicted in Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics, as described in [1], [4], [11], [33].

2.2 System and Adversary Model

Network model–The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in uncast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broad cast communications, symmetric keys are shared among all intended receivers. These keys are established using presaged pair wise keys or asymmetric cryptography.

Communication Model–Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries data bits, whereα/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is _qRbps. Spread spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmissions from jamming. SS provides immunity to interference to some extent (typically20 to 30 dB gain), but a powerful jammer is still capable of jamming data packets of his choosing.

3. Real-Time Packet Classification

In this section, we describe how the adversary can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted in Fig. 2. At the PHY layer, a packet m is encoded, inter leaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinter leaved, and decoded, to recover the original packet m
.

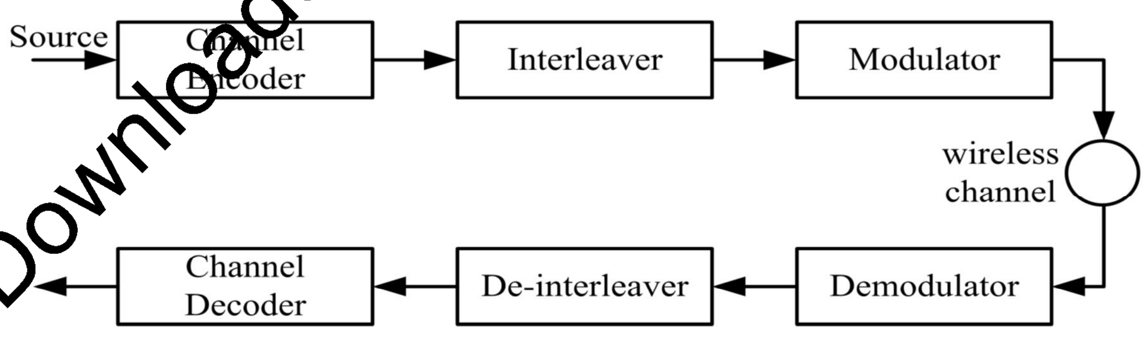

Fig 2. A generic communication system diagram.

The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 2. The channel coding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors.

4 Impact of Selective Jamming

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNETTM Modeller 14.5 [18] to implement selective jamming attack sin two multi-hop wireless network scenarios. In the firsts scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

Selective jamming at the Transport Layer–In the first set of experiments, we setup a file transfer of a 3 MB file between two users A and B connected via a multi-hop route.

Selective Jamming at the Network Layer–In this scenario, we simulated a multi-hop wireless network of 35nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths [19]. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam non-overlapping areas of the network. Three types of jamming strategies were considered: (a) a continuous jammer, (b) a random jammer blocking only a fraction p of the transmitted packets, and (c)a selective jammer targeting route request (RREQ) packets.

5. Hiding Based on Commitments

In this section, we show that the problem of real-time packet classification can be mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments.

5.1 Mapping to Commitment Schemes

Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V while keeping m hidden. Commitment schemes are formally defined as follows [7].

6. Hiding Based on Cryptographic Puzzles

In this section, we present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver [10]. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters.

7. Hiding Based on All-or-Nothing Transformations

In this section, we propose a solution based on All-Or-Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivets to slow down brute force attacks against block encryption algorithms [21].An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.

8. Evaluation of Packet-Hiding Techniques

In this section, we evaluate the impact of our packet-hiding techniques on the network performance via extensive simulations. We used the OPNETTM Modeller 14.5 [18] to implement the hiding sub layer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad-hoc networks.

Impact on real-time systems– Our packet-hiding methods require the processing of each individual packet by the hiding sub layer. We emphasize that the incurred processing delay is acceptable, even for real-time applications. The SCHS requires the application of two permutations.

9 Related Works

Jamming attacks on voice communications have been launched since the 1940s [25]. In the context of digital Communications, the jamming problem has been addressed under various threat models. We present a classification based on the selective nature of the adversary.

9.1 Prior work on Selective Jamming

In [33], Thuente studied the impact of an external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions.

9.2 Non-Selective Jamming Attacks

Conventional methods for mitigating jamming employ some form of SS communications [5], [25]. The transmitted signal is spread to a larger bandwidth following a PN sequence. Without the knowledge of this sequence, a large amount of energy (typically 20-30 dB gain) is required to interfere with an on-going transmission.

Conclusion

An internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets and we showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an on-going transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, crypto graphic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

References

1.]M.Li,I.Kotsiopoulos,andR. Poovendran. Optimal jamming attacks and network defence policies in wireless sensor networks. In *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, pages 1307–1315, Anchorage, AK, USA, May 2007.
2. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. *Aerospace andElectronic Systems Magazine, IEEE*, 24(8):23–30, August 2009.
3. Y. Desmedt. Broadcast anti-jamming systems. *Computer Networks*, 35(23):223–236, February 2001.
4. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES.*Cryptographic Engineering*, pages 235 294, 2009.
5. O. Goldreich. *Foundations of cryptography: Basic applications*. Cambridge University Press, 2004.
6. X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In *Proceedings of INFOCOM*, pages 2536– 2540, 2007.
7. Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *Proceedings of INFOCOM*, San Diego, 2010.
8. R. C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.